CSE 311 Section MR

Midterm Review

Administrivia

Announcements & Reminders

- HW5 (BOTH PARTS)
  - BOTH PARTS were due Wednesday 2/7 @ 11:59pm
  - We will release solutions to HW5 on Ed over the weekend.
  - Homework 5 PT2 feedback/grades are not guaranteed before Monday for late submissions
- HW6 will be released later after the midterm
- Midterm is Coming Next Week!!!
  - Monday 2/12 @ 6:30-8 pm in BAG 131
  - If you cannot make it, please let us know ASAP and we will schedule you for a makeup (makeup form is on Ed)
- Review Session
  - Covering last quarter midterm!
  - Saturday, 2/10 1-3:00pm in CSE2 G20

- **Midterm Logistics on Exams Page**

Proof By Contradiction

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here’s how that works mechanically…

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent statement related to p

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

Then, as a consequence of $\neg p$, we find that both $s \wedge \neg s$ must be true

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

Then, as a consequence of $\neg p$, we find that both $s \land \neg s$ must be true

This gives us an expression of the form:

$$\neg p \rightarrow (s \land \neg s)$$

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

Then, as a consequence of $\neg p$, we find that both $s \wedge \neg s$ must be true

This gives us an expression of the form:

$$\neg p \rightarrow (s \wedge \neg s)$$
$$\neg p \rightarrow F \quad by\ Negation$$

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

Then, as a consequence of $\neg p$, we find that both $s \wedge \neg s$ must be true

This gives us an expression of the form:

$$\neg p \rightarrow (s \wedge \neg s)$$
$$\neg p \rightarrow F \quad \textit{by Negation}$$
$$\mathrm{T} \rightarrow p \quad \textit{by Contrapositive}$$

How Proof By Contradiction Works:

We learned in lecture that you can prove propositions by assuming their logical opposite and then showing that this leads to a contradiction. Here's how that works mechanically…

Let p := proposition we're trying to prove
Let s := a subsequent fact related to p

We begin our proof by supposing, "for the sake of contradiction," $\neg p$ is true.

Then, as a consequence of $\neg p$, we find that both $s \wedge \neg s$ must be true

This gives us an expression of the form:

$$\begin{aligned} &\neg p \rightarrow (s \wedge \neg s) \\ &\neg p \rightarrow F \quad \textit{by Negation} \\ &\mathrm{T} \rightarrow p \quad \textit{by Contrapositive} \\ &p \quad \textit{by Modus Ponens} \end{aligned}$$

Proof By Contradiction and Quantifiers

Oftentimes we will need to prove statements of the form:

$$\forall x P(x)$$

These can be good candidates for proof by contradiction because we can very cleanly negate the statement with its quantifier to get:

$$\exists x \neg P(x)$$

All we have to do to complete this proof via contradiction is suppose the existence of an x that makes $\neg P(x)$ true, and then show that this leads to a contradiction!

Problem 6 – Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.

In predicate logic this could be expressed as $\forall x \forall y (18x + 6y \neq 1)$. HINT: Try negating this statement before writing your proof.

Problem 6 – Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.

Assume, for the sake of contradiction, that there exists integers x and y such that $18x + 6y = 1$.

Problem 6 – Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.

Assume, for the sake of contradiction, that there exists integers x and y such that $18x + 6y = 1$.

This gives us:

$$18x + 6y = 1$$

$$3x + y = \frac{1}{6} \quad \text{Dividing by 6}$$

Problem 6 – Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.

Assume, for the sake of contradiction, that there exists integers x and y such that $18x + 6y = 1$.

This gives us:

$$18x + 6y = 1$$

$$3x + y = \frac{1}{6} \quad \text{Dividing by 6}$$

But wait, this is a contradiction! Integers are closed under multiplication and addition, and so $3x + y$ can't be equal to $\frac{1}{6}$!

Problem 6 – Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.

Assume, for the sake of contradiction, that there exists integers x and y such that $18x + 6y = 1$.

This gives us:

$$18x + 6y = 1$$

$$3x + y = \frac{1}{6} \quad \text{Dividing by 6}$$

But wait, this is a contradiction! Integers are closed under multiplication and addition, and so $3x + y$ can't be equal to $\frac{1}{6}$! This means there can be no integers x and y such that $18x + 6y = 1$. Therefore, the original claim holds via proof by contradiction.

Problem 1: Translation

Problem 1 – Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- soy(x) is true iff x contains soy milk.
- whole(x) is true iff x contains whole milk.
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinated.
- vegan(x) is true iff x is vegan.
- RobbieLikes(x) is true iff Robbie likes the drink x.

Translate each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like = and ≠.

a) Coffee drinks with whole milk are not vegan

b) Robbie only likes one coffee drink, and that drink is not vegan

c) There is a drink that has both sugar and soy milk.

Work on this problem with the people around you.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

a) Robbie only likes one coffee drink, and that drink is not vegan

a) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- $\text{soy}(x)$ is true iff x contains soy milk
- $\text{whole}(x)$ is true iff x contains whole milk
- $\text{sugar}(x)$ is true iff x contains sugar
- $\text{decaf}(x)$ is true iff x is not caffeinate
- $\text{vegan}(x)$ is true iff x is vegan
- $\text{RobbieLikes}(x)$ is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

a) Robbie only likes one coffee drink, and that drink is not vegan

a) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

a) Robbie only likes one coffee drink, and that drink is not vegan

$$\exists x \forall y(\text{RobbieLikes}(x) \land \neg \text{Vegan}(x) \land [\text{RobbieLikes}(y) \rightarrow x = y])$$

a) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

a) Robbie only likes one coffee drink, and that drink is not vegan

$$\exists x \forall y(\text{RobbieLikes}(x) \wedge \neg \text{Vegan}(x) \wedge [\text{RobbieLikes}(y) \rightarrow x = y])$$

Or $\exists x(\text{RobbieLikes}(x) \wedge \neg \text{Vegan}(x) \wedge \forall y[\text{RobbieLikes}(y) \rightarrow x = y])$

a) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \to \neg\text{vegan}(x))$$

a) Robbie only likes one coffee drink, and that drink is not vegan

$$\exists x \forall y(\text{RobbieLikes}(x) \land \neg\,\text{Vegan}(x) \land [\text{RobbieLikes}(y) \to x = y])$$

Or $\exists x(\text{RobbieLikes}(x) \land \neg\,\text{Vegan}(x) \land \forall y[\text{RobbieLikes}(y) \to x = y])$

a) There is a drink that has both sugar and soy milk.

$$\exists x\big(\text{sugar}(x) \land \text{soy}(x)\big)$$

Problem 1 – Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- soy(x) is true iff x contains soy milk.
- whole(x) is true iff x contains whole milk.
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinated.
- vegan(x) is true iff x is vegan.
- RobbieLikes(x) is true iff Robbie likes the drink x.

Translate the following symbolic logic statement into a (natural) English sentence. Take advantage of domain restriction.

$$\forall x([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Work on this problem with the people around you.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \land \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \land \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Every decaf drink that Robbie likes has sugar.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Every decaf drink that Robbie likes has sugar.

Statements like "For every decaf drink, if Robbie likes it then it has sugar" are equivalent, but only partially take advantage of domain restriction.

Problem 2: English Proof

Problem 2- Even Steven

Prove that for all integers k, k(k +3) is even.

Recall that Even(x) := $\exists$k(x = 2k) and Odd(x) := $\exists$k(x = 2k + 1)

(a) Let your domain be integers. Write the predicate logic of this claim.

Problem 2- Even Steven

Prove that for all integers k, k(k +3) is even.

Recall that Even(x) := $\exists$k(x = 2k) and Odd(x) := $\exists$k(x = 2k + 1)

(a) Let your domain be integers. Write the predicate logic of this claim.

$\forall$k(Even(k(k+3)))

What kind of proof technique might we need?

Problem 2- Even Steven

Prove that for all integers k, k(k +3) is even.

Recall that Even(x) := $\exists k(x = 2k)$ and Odd(x) := $\exists k(x = 2k + 1)$

(a) Let your domain be integers. Write the predicate logic of this claim.

$\forall k(\text{ Even}(k(k+3)))$

What kind of proof technique might we need?

This looks like a proof by cases!

Problem 2- Even Steven

(b) Write an English proof for this claim.

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let **k** be an **arbitrary** integer

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let **k** be an **arbitrary** integer

Case 1: k is even

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let **k** be an **arbitrary** integer

Case 1: k is even

By the definition of even, k = 2j for some integer j

So substituting for k into k(k + 3):

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let **k** be an **arbitrary** integer

Case 1: k is even

By the definition of even, k = 2j for some integer j

So substituting for k into k(k + 3):

$$k(k+3) = (2j)(2j+3) = 2(2j^2 + 3j)$$

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let **k** be an **arbitrary** integer

Case 1: k is even

By the definition of even, $k = 2j$ for some integer j

So substituting for k into $k(k + 3)$:

$$k(k+3) = (2j)(2j+3) = 2(2j^2 +3j)$$

$k(k + 3) = 2n$, where $n = (2j^2 + 3j)$ and n is an integer since j is an integer and integers are closed under addition and multiplication.

So, by definition of even, $k(k + 3)$ is even.

Problem 2- Even Steven

(b) Write an English proof for this claim.

Case 2: k is odd

Problem 2- Even Steven

(b) Write an English proof for this claim.

Case 2: k is odd

By the definition of odd, $k = 2j + 1$ for some integer j

So substituting for k into $k(k + 3)$:

Problem 2- Even Steven

(b) Write an English proof for this claim.

Case 2: k is odd

By the definition of odd, $k = 2j + 1$ for some integer j

So substituting for k into $k(k + 3)$:

$$k(k+3) = (2j+1)(2j+1+3) = (2j+1)(2j+4) = 4j^2 + 10j + 4 = 2(2j^2 + 5j + 2) = 2(2j+1)(j+2)$$

Problem 2- Even Steven

(b) Write an English proof for this claim.

Case 2: k is odd

By the definition of odd, $k = 2j + 1$ for some integer j

So substituting for k into $k(k + 3)$:

$$k(k+3) = (2j+1)(2j+1+3) = (2j+1)(2j+4) = 4j^2 + 10j + 4 = 2(2j^2 + 5j + 2) = 2(2j+1)(j+2)$$

$k(k + 3) = 2n$, where $n = (2j + 1)(j + 2)$ and n is an integer since j is an integer and integers are closed under addition and multiplication.

So, by definition of even, $k(k + 3)$ is even.

Problem 2- Even Steven

(b) Write an English proof for this claim.

Let k be an arbitrary integer

Case 1: k is even

By the definition of even, k = 2j for some integer j

So substituting for k into k(k + 3):

$$k(k+3) = (2j)(2j+3) = 2(2j^2 +3j)$$

k(k + 3) = 2n, where n = (2j2 + 3j) and n is an integer since j is an integer and integers are closed under addition and multiplication.

So, by definition of even, k(k + 3) is even.

Case 2: k is odd

By the definition of odd, k = 2j + 1 for some integer j

So substituting for k into k(k + 3):

$$k(k+3) = (2j+1)(2j+1+3) = (2j+1)(2j+4) = 4j2 +10j+4 = 2(2j^2 +5j+2) = 2(2j+1)(j+2)$$

k(k + 3) = 2n, where n = (2j + 1)(j + 2) and n is an integer since j is an integer and integers are closed under addition and multiplication.

So, by definition of even, k(k + 3) is even.

These cases are exhaustive, so the claim that k(k + 3) is even must hold.

Since k was arbitrary, the claim holds for all k.

Problem 4: Induction

Problem 4 – Induction

For any $n \in \mathbb{N}$, define S_n to be the sum of the squares of the first n positive integers, or $S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Work on this problem with the people around you.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "". We show $P(n)$ holds for (some) n by induction on n.

Base Case: $P(b)$:

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for (some) n by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(b)$:

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= \\
&= \cdots \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned} S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\ &= \cdots \\ &= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1) \end{aligned}$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned} S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\ &= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\ &= \cdots \\ &= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1) \end{aligned}$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\frac{1}{6}k(2k+1) + (k+1)) \\
&= \frac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \cdots \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2.$

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 4 – Induction

$S_n = 1^2 + 2^2 + \cdots + n^2$.

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\
&= \tfrac{1}{6}(k+1)(k+2)(2k+3) \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 3: Number Theory

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2\%p = 1$.

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p-1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Work on this problem with the people around you.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[\left(y \equiv 1 \pmod{p}\right) \rightarrow \left(y^2 \equiv 1 \pmod{p}\right)]$

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$.
…
$y^2 \equiv 1 \pmod{p}$.
Since y is arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod{p}$.
$\ldots y^2 \equiv 1 (\text{mod } p)$
Since y is arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod{p}$.
Simplifying, we have $y^2 \equiv 1 (\text{mod } p)$
Since y is arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don’t use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

$\ldots$

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x - 1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x - 1)$.

…

$x^2 \equiv 1 \pmod{p}$.

Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x - 1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x - 1)$.
By multiplying both sides of $pk = (x - 1)$ by $(x + 1)$, we have $pk(x + 1) = (x - 1)(x + 1)$.
…

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x - 1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x - 1)$.
By multiplying both sides of $pk = (x - 1)$ by $(x + 1)$, we have $pk(x + 1) = (x - 1)(x + 1)$.
Rearranging the equation, we have $p(k(x + 1)) = (x - 1)(x + 1)$.
…

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x-1)$.
By multiplying both sides of $pk = (x-1)$ by $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

Since $(x-1)(x+1) = x^2 - 1$, by replacing $(x-1)(x+1)$ with x^2-1, we have
$p(k(x+1)) = x^2 - 1$

…
$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x-1)$.
By multiplying both sides of $pk = (x-1)$ by $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

Since $(x-1)(x+1) = x^2 - 1$, by replacing $(x-1)(x+1)$ with $x^2 - 1$, we have $p(k(x+1)) = x^2 - 1$

Note that since k and x are integers, $k(x+1)$ is also an integer. Therefore, by the definition of divides, $p \mid x^2 - 1$.
$\ldots x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that $pk = (x-1)$.
By multiplying both sides of $pk = (x-1)$ by $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

Since $(x-1)(x+1) = x^2 - 1$, by replacing $(x-1)(x+1)$ with $x^2 - 1$, we have $p(k(x+1)) = x^2 - 1$

Note that since k and x are integers, $k(x+1)$ is also an integer. Therefore, by the definition of divides, $p \mid x^2 - 1$.
Hence, by the definition of Congruences, $x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that
$x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x \% p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x \% p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that
$x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that
$x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2\%p = 1$

c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that
$x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
Since $(x - 1)(x + 1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x - 1)(x + 1)$, we have $p \mid (x - 1)(x + 1)$
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that
$x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
Since $(x-1)(x+1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x-1)(x+1)$, we have $p \mid (x-1)(x+1)$
Note that for an integer p, if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x \% p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x \% p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
Since $(x-1)(x+1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x-1)(x+1)$, we have $p \mid (x-1)(x+1)$
Note that for an integer p, if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
In this case, since p is a prime number, by applying the rule, we have $p \mid (x-1)$ or $p \mid (x+1)$.

$\ldots x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

Let p be a prime number at least 3 and let x be an integer such that $x^2 \% p = 1$

c) From part (a), we can see that $x \% p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x \% p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x - 1)(x + 1)$
Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
Since $(x - 1)(x + 1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x - 1)(x + 1)$, we have $p \mid (x - 1)(x + 1)$
Note that for an integer p, if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
In this case, since p is a prime number, by applying the rule, we have $p \mid (x - 1)$ or $p \mid (x + 1)$.

Therefore, by the definition of Congruences, we have $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

That’s All, Folks!

Thanks for coming to section this week!
Any questions?